

09/770,525

Page 2 of 8

This listing of claims will replace all prior versions and listings of claims in the application:

**Listing of Claims:**

1-22. (Canceled)

23. (Currently Amended) A security system for a computer network, the network having a plurality of devices connected thereto, the security system comprising:

(a) a security subsystem connected to at least some of the devices in the network, the security subsystem configured to monitor activities of the at least some devices on the network and detect attacks on the at least some devices;

(b) a master system which monitors the integrity of the security subsystem and registers information pertaining to attacks detected by the security subsystem; and

(c) a first secure link connected between the security subsystem and the master system, the master system monitoring the integrity of the security subsystem and receiving the information pertaining to the attacks through the first secure link,

wherein the master system further monitors whether the security subsystem responds to the master system, the master system taking action if no response is detected.

24. (Canceled)

25. (Previously Presented) The system of claim 23 wherein the master system does not take direction from the security subsystem.

26. (Previously Presented) The system of claim 23 further comprising:

(d) a second secure link connected between the master system and the network which enables data communication from the master system to the network for issuing instructions to the network devices.

27. (Previously Presented) The system of claim 26 wherein the instructions are issued if the first secure link is severed or compromised.

10211287.1

09/770,525

Page 3 of 8

28. (Previously Presented) The system of claim 23 wherein the master system is hierarchically independent from the security subsystem.

29. (Previously Presented) The system of claim 23 wherein the security subsystem is hierarchically subordinate to the master system.

30. (Previously Presented) The system of claim 23 wherein the first secure link is defined by a virtual private network (VPN) tunnel.

31. (Canceled)

32. (Previously Presented) The system of claim 23 wherein the master system further comprises a pseudo-attack generator which generates attacks on the network, the security subsystem detecting such attacks and sending expected replies to the master system when its integrity is intact, the master system detecting whether the expected replies are received in response to a pseudo-attack to determine whether the integrity of the subsystem has been compromised.

33. (Currently Amended) A security system for a computer network, the network having a plurality of devices connected thereto, at least some of the devices having security-related functions, the security system comprising:

- (a) a security subsystem associated with at least some of the devices in the network which tests the integrity of the security-related functions;
- (b) a master system which monitors the integrity of the security subsystem and receives and stores results of the integrity testing of the devices having security-related functions; and
- (c) a secure link connected between the security subsystem and the master system, the master system monitoring the integrity of the security subsystem and receiving the results of the integrity testing of the devices having security-related functions through the first secure link, wherein the security subsystem or the master system initiates countermeasures upon detecting that the integrity of a device having security-related functions has been compromised.

10211287.1

09/770,525

Page 4 of 8

34. (Canceled)

35. (Previously Presented) The system of claim 33 wherein the security subsystem tests the integrity of the security-related functions by generating pseudo-attacks on the devices having security-related functions.

36. (Canceled)

37. (Currently Amended) The system of claim ~~36~~ 33 wherein the countermeasures include restricting or disabling access to the network or a device in the network.

38. (Previously Presented) The system of claim 33 wherein the master system further comprises a pseudo-attack generator which generates attacks on the network, the security subsystem detecting such attacks when functioning properly, the master system comparing the pseudo-attacks made on the network to the attacks actually detected by the subsystem, the master system thereby determining whether the integrity of the subsystem has been compromised.

39. (Previously Presented) The system of claim 33 wherein the secure link is defined by a virtual private network (VPN) tunnel.

40. (Previously Presented) The system of claim 33 wherein at least one of the devices having security-related functions is a firewall.

41. (Previously Presented) The system of claim 33 wherein at least one of the devices having security-related functions is a network intrusion detection system.

42. (New) A security system for a computer network, the network having a plurality of devices connected thereto, the security system comprising:

(a) a security subsystem connected to at least some of the devices in the network, the security subsystem configured to monitor activities of the at least some devices on the network and detect attacks on the at least some devices;

10211287.1

09/770,525

Page 5 of 8

(b) a master system which monitors the integrity of the security subsystem and registers information pertaining to attacks detected by the security subsystem; and

(c) a first secure link connected between the security subsystem and the master system, the master system monitoring the integrity of the security subsystem and receiving the information pertaining to the attacks through the first secure link,

wherein the security subsystem or the master system initiates countermeasures upon detecting that the integrity of the at least some devices on which an attack has been detected has been compromised.

10211287.1